SERVICE OPERATIONS MANUAL
REMOTE MANAGED SERVICE

emPSN – Schools Version 2.8

SOM Table of Contents

1 DOCUMENT CONTROL

Document Reference	Service Operations Manual for emPSN Schools (End Users)
Document Creator	Ian Martin, Transition Programme Manager
In Life Document Owner	Andy Ball Client Services Manager
Date of Current Issue	January 2023
Version No	External 2.8
Change History	1.0 First Issue of SOM Main Body
	1.6 Added Security Incident Management Procedure (Embedded document)
	1.7 Added Third Party Filtering information
	1.8 Added Major incident management process to section 5.2
	1.9 Reviewed content
	2.0 Remove of RM details
	2.1 Details of emailed updates (section 5.2)
	2.2 Change from SMC to CSOC
	2.3 Add FTTP SLA's
	2.4 Amendments to Client Principle contacts details and incident escalation contact names
	2.5 Expanded Change criteria detail in section 6.2
	2.6 Amendments to contacts
	2.7 Nasstar re-brand, update of Nasstar contacts
	2.8 Reviewed content

Document Accepted by:

Nasstar Service Transition Manger	TBC
Nasstar Operations Manager	Tim Hemsley
Nasstar CNOC Team Leader	Kieran Marsden / Adam Cramer
Nasstar Change Team Manager	Nicki Hart
Nasstar Client Services Team Leader	Jacky Dunne
emPSN Operations Manager	Ric Stevenson

Document Distributed to:

Nasstar Client Services Manager	Andy Ball
Nasstar Lifecycle Consultant	Michael Weston
Nasstar CNOC Secure Drive	emPSN End User Customer Folder
End User Customers	Head Teacher or School Business Contact
emPSN Operations Manager	Ric Stevenson

2 INTRODUCTION

2.1 Purpose and Scope of Document

The purpose of this document is to record the catalogue of Managed Services contracted by End User Customers (Customer) under the East Midlands Public Sector Network (emPSN) infrastructure agreement, and to hold information relevant to the delivery of the services as described in the contracted Service Description. The intended audience for this document are the operational communities of Nasstar and the Customer, and emPSN Infrastructure Limited (ICo).

This is a working document and is subject to review and change by agreement between emPSN and Nasstar throughout the life of the contract in order that it remains accurate and relevant to the services being provided. This is not a contractual document. With respect to any conflicts between this document and the requirements set out under the contract, the emPSN contract schedule will take precedence.

The key goals of this document are as follows:

- To provide a catalogue of the Managed Service elements provided to the Customer by Nasstar under the scope of the contracted service
- To describe for the benefit of the operational communities of Nasstar and the Customer, the relevant information which they require to interact during the delivery of the service

Other PSN Framework Providers

Nasstar are a provider of:

i) WAN Connectivity Services
ii) Education Application Services

Other companies are members of the emPSN Framework Agreement and you may have contracted Education Application Services directly from them.

If you suffer a fault relating to an Education Service provided by another party, please contact them in the first instance to report the fault relating to a service that they provide.

Please see the emPSN customer portal for guidance to help you decide whether the cause of fault is likely to be due to the Connectivity Service provided by Nasstar, or the Application Service provided by another party.

If you are in doubt about the cause of a fault, you can call the Nasstar incident reporting number detailed later in this document. You will be asked a series of questions to try and identify the cause of your problem. Nasstar will then diagnose the cause and assign responsibility for the fault repair either to our own teams or to those of your Education Service Provider.

3 KEY CONTACT DETAILS

3.1 Customer key personnel contact details

Contact details for End User customers will be retained on the emPSN portal. Nasstar In Life Services will retain a controlled working copy of this information.

3.2 Nasstar key personnel contact details

Name	Role	Tel. No.	E-Mail
Network Support	24x7x365 Point of Contact	0845 122 6873	networksupport.@nasstar.com
Active Manager	NOC Team Leader	0845 122 6873	networksupport.@nasstar.com
Active Manager	Operations Manager	0845 122 6873	networksupport.@nasstar.com

3.3 Supported customer sites:

The definitive list of supported customer equipment and services is maintained on the emPSN portal for real time review by Customer which is available at the address: https://nasstar.service-now.com/serviceportal

3.4 Site Access Arrangements

Arrangements for customer site access will always be made through the site main contact number. If the contact number is not answered, eg outside school hours, Nasstar will attempt to contact the customer again during the next business day.

Site Address	Access Arrangements
WAN Edge Site	Nasstar will request access via the Customer Main Contact No Nasstar will normally provide: - 5 days advance notice for planned works (This will not be feasible when responding to an incident, eg to repair the failure of a circuit or CPE equipment) - Name of visiting engineer - Date and time of visit

4 SERVICE CATALOGUE

4.1 Service Period

The service period for Customer is as follows:

Managed Service Operating Hours	24 x 7 x 365
Hardware Support Operating Hours	As per line item details in Nasstar contract management system (viewable from the emPSN customer portal)

4.2 Managed Service Catalogue

The following is a summary of the services subscribed to by Customer which combine to make the Managed Service offering.

Service Scope	Description	Contractual Status
Network Support	A 24x7x365 Service Desk function	Included
Managed Infrastructure Monitoring	Nasstar shall provide 24x7 monitoring of the Communications Infrastructure status, performance against pre-defined thresholds or alerts / events that indicate a potential to impact the service.	Included
Incident Management	Incident Management providing ownership and resolution of Incidents	Included
Hardware Support	Replacement of faulty Hardware and the provision of updated Software	Included
Change Management	Implementation of Requests for Change as detailed in this document,	Included
Configuration Management	Maintenance of documentation, regular backup of device configurations and management of controlled access to the Communications Infrastructure elements	Included
Lifecycle Services	Access to summary information on the performance, capacity and availability of the communications Infrastructure via the emPSN portal	Included
emPSN Portal	Access to service related information via the emPSN customer portal	Included

4.3 Managed Service Infrastructure and Services

The following table identifies the scope of technologies and locations to which the above catalogue of Managed Services will be provided.

PSN Component	Solution Scope
Wide Area Network (Managed Service and Support Service)	- Access circuit to the nearest emPSN exchange - Customer premises termination equipment - Core Firewall services
Private DSL Network If Applicable (Managed Service and Support Service)	- Provided between specified edge sites and the emPSN datacentre
Application Services If Applicable	- Netsweeper and esafety4schools provide application services for schools

The potential WAN access methods are described below:

WAN Access Option	WAN Speed	Delivery Medium	Availability
Ethernet	Variable	Private DSL	Universally Available
Ethernet	2-20Mbps	Copper (MPF)	Where local exchange is unbundled
Ethernet	2-80Mbps	FTTC	Universally Available
Ethernet	80-330 Mbps	FTTP	Dependant on supplier rollout
Ethernet	10-100Mbps	Fibre	Universally Available
Ethernet	1Gbps	Fibre	Universally Available

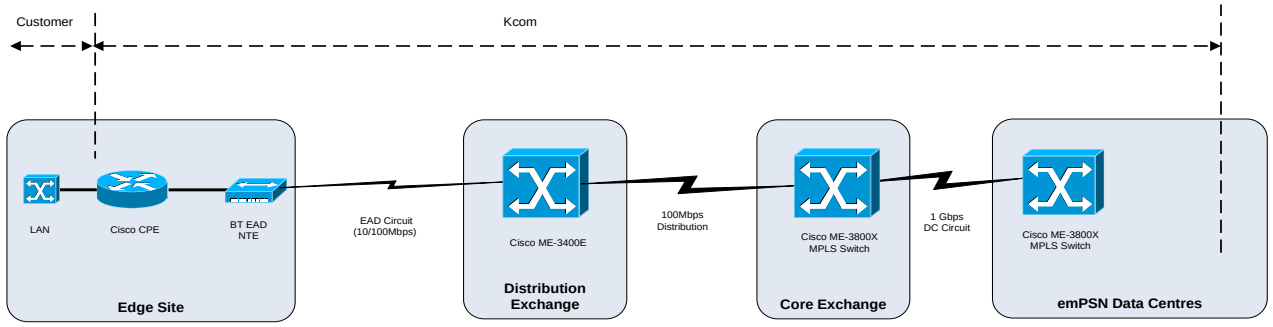
Connections will be based on the methods above, with varying numbers of MPF pairs depending on the nature of the edge site and distance from the serving exchange.

4.4 WAN Service Boundaries

The drawing below illustrates who is responsible for each element.

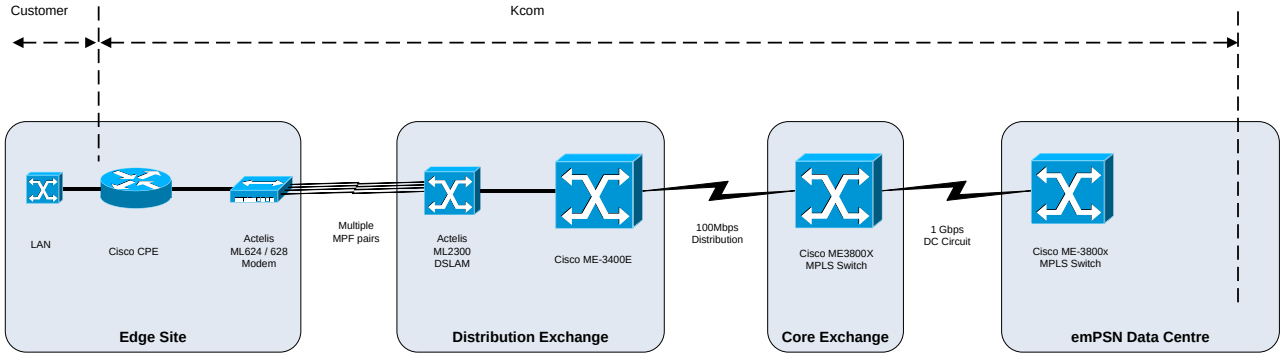
Ethernet Connected Site

The Managed Service demarcation point at an EAD connected site is the LAN interface of the customer edge WAN router.



MPF or FTTC Connected Site

The Managed Service demarcation point at a MPF or FTTC connected site is the LAN interface of the customer edge WAN router.



Nasstar shall provide 24x7 monitoring of the Communications Infrastructure status, performance against pre-defined thresholds or alerts / events that indicate a potential to impact the service. Nasstar shall raise an Incident where the pre-defined threshold is exceeded or an alert / event is detected.

In the event that an edge site CPE failure is detected from the distribution network, the ticket will be passed to the Customer to perform edge site diagnostics as described in this SOM prior to the incident being progressed by Nasstar. This is to ensure that the root cause of the incident is not due to customer provided dependencies, e.g. edge site power availability.

4.5 emPSN Portal Access

Nasstar shall provide the Customer with access via the internet to the emPSN Customer Portal on a 24x7 basis. The emPSN Portal will be accessed at: https://nasstar.service-now.com/serviceportal

To become a Portal user email the Nasstar Network Support at networksupport.@nasstar.com and request a Portal access form.

5 OPERATE SERVICES – INCIDENT MANAGEMENT

5.1 Incident Management Reporting Point of Contact

Name	Role	Tel. No.	E-Mail
Network Support	24x7x365 Point of Contact	0845 122 6873	networksupport.@nasstar.com

5.2 Incident Management Reporting Process

Incidents shall be accepted either:

- By telephone to the contact number above
- Online (via the emPSN Portal)
- By email
- Or as an event/alarm from Nasstar's Management Systems and determined by Nasstar to be an Incident

Nasstar will log all Incidents raised by telephone or the online portal within 15 minutes of receipt and allocate a unique reference number.

emPSN acknowledges that Nasstar does not have an automated facility for logging emails, Nasstar will log all Incidents raised by email as soon as reasonably practicable and will allocate a unique reference number. Nasstar therefore recommends that incidents are reported by telephone whenever possible.

For updates to incident tickets, emailed updates into the network support will be actioned upon as soon as reasonably practicable. If the emailed update is urgent best practice would be to follow up with a telephone call to the network support to prompt actions necessary. Out of hours emails and calls are routed to the CSOC 24/7 operation.

The Customer shall be asked to provide the following key information when raising an incident:

- The customer site emPSN identification number
- Organisation name and post code of the affected site
- Caller's name, telephone number and email address
- Caller's own Incident reference number if available
- Further information will be requested to help diagnose the cause of the incident

The Nasstar Network Support will ask a number of initial triage questions to determine the nature of the incident. These will include checks to ensure that Incidents relating to the environment e.g. power are resolved by Customers and such Incidents are not raised as Incidents with Nasstar. Further information about Customer responsibilities is contained in the appendix to this document.

Third Party Filtering: Should you encounter an issue relating to your filtering service in the first instance please contact your third party filtring company. If they cannot resolve the issue then please contact the Nasstar Network Support to raise an incident ticket.

These are typically but not exclusively one of the following:

ES4S
Capital Bytes
Netsweeper
LGfL

Ticket Management:

Where a P1 Incident occurs a master ticket should be raised against a Core or Exchange site, with subsequent individual tickets then being raised against every single site reporting an issue. Each of these subsequent tickets should always refer back to the master ticket therefore ensuring any reporting or service credit payments reflect the correct time period.

Where an incident occurs that is not obviously a P1 and incident ticket are raised against one or several customer sites then at the point it becomes evident that there is a P1 issue a master ticket should be created against the Core or Exchange site and this ticket should reflect the time that the first site ticket was raised, with each of the individual site tickets being updated with the new master ticket reference therefore ensuring any reporting or service credit payments reflect the correct time period.

Major Incident Management Process

A Major Incident is defined as one that is assessed by the Service Operations Centre as a Priority 1. Priority will be determined from a combination of the urgency and impact of the incident.
Nasstar will use their own Major Incident Management procedure, IMS2232, unless stated otherwise and agreed by the customer.

5.3 Incident Prioritisation

Nasstar shall assign each Incident a Priority based on impact, severity and Urgency as detailed in the table below, a Priority 1 or 2 incident will usually only be assigned for core network incidents that are affecting a number of customer sites:

Priority 1 (P1)	For any Incident to be assigned a Priority 1, the end customer must guarantee Nasstar access where necessary to the Communications Infrastructure for diagnostic purposes A significant part of the Communications Infrastructure at multiple Sites is down, with the potential of causing critical impact to the end customer business operations if service is not restored quickly. The end customer is willing to commit substantial resources around the clock if required to resolve the situation.

Priority 2 (P2)	

	The Communications Infrastructure is severely degraded, impacting significant aspects of Customer business operations. The end customer is willing to commit full-time resources during business hours if required to resolve the situation
Priority 3 (P3)	The Communications Infrastructure performance is degraded. Functionality is noticeably impaired, but most business operations continue.
Priority 4 (P4)	The end customer needs information concerning product capabilities, installation advice, or basic product configuration data

Nasstar shall perform initial diagnostics as detailed below:

P1, P2, P3	Nasstar shall perform initial diagnostics and provide the end customer (and, for high priority Incidents, ICo, where previously agreed and documented in the SOM) with a status report within the target diagnostics time as listed in the Service Operations Manual. Nasstar shall investigate and attempt to resolve the problem remotely, either via the network management platform or by telephone diagnostics, deploying field engineers or spares logistics where appropriate.
P4	For Priority 4 Incident reports, Nasstar shall provide an initial response as listed in the Service Operations Manual.

5.4 Incident Service Level Response and Resolution

For all Incidents the resolution targets shall be as detailed below.

Component Type	Initial Response Target	Commence Diagnostics Target	Incident Resolution Target
Core WAN	15 minutes	30 minutes	6 Hours
MPF	15 minutes	30 minutes	6 Hours
Fibre and EFM Ethernet Circuit (10Mbps, 100Mbps & 1Gbps)	15 minutes	30 minutes	6 Hours
Fibre to the Cabinet (GEA FTTC and pFTTC)	15 minutes	30 minutes	6 Hours
Fibre to the Premise (FTTP)	15 minutes	30 minutes	6 Hours
Edge Site - ADSL	15 minutes	30 minutes	48 Hours
Edge Site – Resilient	15 minutes	30 minutes	6 Hours

Nasstar shall use reasonable endeavours to identify and implement any workarounds required to restore service as quickly as possible until a permanent solution has been identified.

Where access to a site is restricted by the end user, this may impact on the incident resolution target clear time.

NASSTAR INCIDENT ESCALATION PROCESS

Escalation	Elapsed Time	Escalation Contact – Managed Services Customers
Level 1	1 hour before SLA target time	CNOC Network Support
Level 2	30 minutes before SLA target time	CNOC Team Leader
Level 3	1 hours past the SLA target time	CNOC Duty Manager (Client Manager as additional)
Level 4	2 hours over the SLA target time	CNOC Head of Service Operations/Duty Director

If a site believes Nasstar have failed to perform to the contracted SLA then complaints can be progressed via complaints@nasstar.com

All Nasstar escalation contacts will be available via the Network Support on 0845 122 6873

6 OPERATE SERVICES - CHANGE MANAGEMENT

6.1 Change Request Process

A Request for Change means a request raised by a customer for a modification to the Communication Infrastructure which can be completed remotely and does not require resources or equipment such as:

- Consultancy, Project Management or Implementation resources.
- Additional Hardware, Software or Network Bandwidth.

Requests for Change that require resources or equipment as detailed above shall be processed as a Service Request.

Requests for Change shall be accepted via the emPSN online portal https://nasstar.service-now.com/serviceportal

Each Request for Change shall be allocated a unique Change Request number, and implementation will conform to the emPSN Technical Change Request process. Customers shall be able to track the status of a validated Request for Change via the emPSN Customer Portal.

Where the Change Request is for an ACL modification, the request must be accompanied with authorisation from the Head Teacher of the associated school / academy. On receipt of the request this will need to be forwarded to emPSN.

6.2 Change Classification

Validated Requests for BAU none Firewall Change shall be allocated one of the following classifications:

Category	SLA	Risk	Maximum Number of Requests Allowed
Planned Changes			
Major	A minimum of 14 days to implement plus appropriate planning time	High	N/A
Significant	7 Days to implement	Medium	N/A
Minor	1 Day to implement	Low	N/A
Exceptional Changes			
Expedite	As soon as practicable	To be defined on submission of request	Must not be used repeatedly to bypass SLAs for normal process
Incident Related (P1 and P2 incidents only)	Immediate implementation	To restore service during an Incident	N/A

Validated Requests for Firewall Change shall be allocated one of the following classifications:

Category	SLA	Risk	Maximum Number of Requests Allowed
Planned Changes			
Major	A minimum of 14 days to implement plus appropriate planning time	High	N/A
Significant	7 Days to implement	Medium	- RFI for a customer's configuration - Significant number of rule alterations on a completed form > 10 hosts and/or ports
Minor	1 Day to implement (24 hours)	Low	- Minor number of rule alterations on a completed form <= 10 hosts and/or ports
Exceptional Changes			
Expedite	As soon as practicable	To be defined on submission of request	Must not be used repeatedly to bypass SLAs for normal process
Incident Related (P1 and P2 incidents only)	Immediate implementation	To restore service during an Incident	N/A

Nasstar Change control will review the change form and information submitted by the customers. The details will be checked for Completeness, if information supplied meets the minimum requirement to fulfil the request then the target time will be applied to the Change ticket.
If the form is ambiguous or incomplete then Nasstar Change will contact the customer requesting vendor details, Web links, rule information. If it is apparent that the customer does not have this information then Nasstar will offer the customer assistance from emPSN.

6.3 Authorised Change Requestors

The personnel authorised by the customer to make Requests for Change will be issued emPSN portal user accounts with the appropriate privilege to raise RFCs.PSN Change Approval Process
If the scope of the Customer RFC does not fall into the pre-defined Minor category, then Nasstar will plan the RFC, and will provide the PSN Change Approval Board with a CAB "Approval Request". Nasstar will not proceed with the execution of the RFC until the PSN CAB formally approves the request. On receipt of PSN CAB approval, Nasstar will execute RFCs within the SLA periods defined in the Service Description.

6.4 Outage Notifications

In the event that an interruption to services is necessary, typically arising from advance notification by a third party supplier of a circuit outage, then Nasstar will provide notification via email to the customer.

Customer will forewarn Nasstar of planned outages that may affect the communications infrastructure at edge sites by email to networksupport@nasstar.com

For example: If customers are switching power off due to building works or holidays

6.5 Service Request Process

Service Request means a general request for information relating to the Communication Infrastructure or Request for Change to the Communication Infrastructure that requires resources or equipment such as:

- Consultancy, Project Management or Implementation resources.
- Additional Hardware, Software or Network Bandwidth.

Where additional resources or equipment are required additional charges shall apply. Service Requests shall be submitted as described below.

Nasstar will provide a price for each Service Request as described in the Service Catalogue and the Price Book. Upon acceptance by ICo or the appropriate end customer, the Change Control procedure will be followed as described in Schedule 14 Part A of the emPSN Infrastructure Agreement.

Service Requests shall be accepted by email to salessupportdesk@nasstar.com and the Service Request shall include:

- Contact details for a suitable contact who can respond to any queries with respect to the Service Request
- A detailed description of the requirements
- A list of any caveats or pre requisites
- Priority with respect to other outstanding Service Requests
- Timescales for implementation

On receipt of the service request to the Sales Support Desk, an automated email will be returned with a Call Reference. The Call Reference will be required on any further correspondence relating to that request.

Service Requests shall be passed to the Sales Support Desk and the Service Request will be processed as follows:

- The Sales Support Desk shall mobilise the appropriate resources to work with Customer to understand the requirement
- Once the requirement is understood a document shall be provided to Customer by the Sales Support Desk detailing the proposed solution, any dependencies and assumptions and associated charges
- Once the document and charges are agreed a Contract Change Notice shall be signed by both parties

Upon receipt by Nasstar of a completed Contract Change Notice Nasstar shall undertake the Service Request as agreed in the Contract Change Notice, following the normal Change Management process as required to request authorisation to implement changes to the production network.

The Sales Support Desk hours are 8am – 5pm, Monday – Friday

For escalations relating to service requests, please contact the Sales Support Desk Manager in the first instance on telephone number 0330 3333030. If any further escalation is require please contact Client Service Desk 0808 1560024.

6.6 Incident Related Change

All incident-related changes are initially recorded in the incident ticket. Nasstar will then raise a retrospective RFC, allocating the appropriate Significant or Minor classification.

In the event of failures of individual MPF circuits within a bundle, that reduce the capacity available to an edge site but do not cause a complete service outage, Nasstar will manage the circuit repair and will then advise the Customer that the service is ready to be re-trained to restore full capacity. The Customer will notify Nasstar whether this should be undertaken immediately or scheduled for outside normal business hours.

6.7 Network Security Arrangements

All Nasstar provided customer premises equipment will be secured by Nasstar and remote management access will not be provided to the customer.

6.8 Software Changes

Software Updates / Upgrades

Minor Upgrades or Minor Versions of software upgrades will be implemented by Nasstar where required to resolve Service Impacting Incidents subject to no additional Hardware being required. For the avoidance of doubt if additional Hardware is required this will be subject to additional charges and Nasstar agreement to provide such.

Where any planning resources, implementation resources, Hardware or Software are required (other than where a device is subject to a Service Impacting Incident) in order to implement an Upgrade this will be subject to additional charges and shall follow the process for Service Requests.

Software Vulnerabilities
From time to time manufacturers may discover Software vulnerabilities and those vulnerabilities may be exploited to interrupt or reduce operation or provide a mechanism to allow unauthorised access to the Communications Infrastructure or services provided by the Communications Infrastructure. Where the end customer requires or Nasstar recommends software to be upgraded as the result of Software vulnerabilities additional charges may apply as detailed under the Service request process.

8. COMPLIMENTS AND COMPLAINTS

Nasstar make every effort to ensure that our customers are happy with the level of service, and the products and services they receive from us. However, despite our best efforts, things can go wrong. We take customer complaints very seriously and aim to resolve them quickly and efficiently.

If you'd like to submit a complaint, please forward the details to your service management representative as well as to complaints@nasstar.com

If you would like further information, please visit Complaints Procedure | Nasstar

Appendix 1 – Change classification descriptions

The following section provides high-level descriptions and examples of RFCs and how they will be classified in terms of Urgency Category. Where the RFC is not listed in this Managed Service Change Catalogue it will be treated as a Service Request.

Major Request for Change

Requests classified as Major will typically require additional resources or hardware and software and unless agreed otherwise by Nasstar will be dealt with as a Service Request.

Significant Request for Change

Requests classified as Significant typically do not require additional resources or hardware and software, and will therefore usually be accepted by Nasstar for execution as in life changes. If additional resources are required, these will be dealt with as a Service Request.

Significant RFCs typically result in impact to a single device and affect a small number of users e.g. an access layer switch or small remote site. Significant Changes will be designed by Nasstar and submitted to the Customer Change Advisory Board for approval before remote execution by Nasstar.

Examples of Significant RFCs include

WAN
Apply OS/IOS Update or Patch
Change IP route redistribution

Minor Request for Change

Requests classified as Minor can typically be completed remotely without any additional resources or hardware and software. Minor Requests for Change typically result in low impact where users would not realise the Change has happened. Typically Minor Requests for Change are standard design and pre-approved by ICo CAB for implementation.

The following RFCs will be accepted by Nasstar for execution as in life changes. These changes are typically pre-approved by the customer Change Advisory Board for execution by Nasstar as soon as practicable on receipt of a customer RFC.

WAN
Change Interface Characteristics e.g. Speed / Duplex mode
Add / remove port to/from existing VLAN
Apply ACL
Enable / Disable / Label Port

Nasstar Expedite/Customer Emergency Request for Change

Requests classified as Expedite relate to urgent unforeseen customer business needs only. Nasstar assumes no liability for loss or damage sustained by Customer as a result of expediting a RFC. In addition if there is any loss of service to the Communications Infrastructure as a result of expediting a RFC this will be excluded from any service level calculations.

APPENDIX 2 – EDGE SITE TRIAGE PROCESS

emPSN Customers have the following obligations arising from the emPSN Framework Agreement

- Having regard to the nature of the equipment, ensure all the Communications Infrastructure installed on end customer premises, including Nasstar's Equipment, is maintained in an environment suitable for its operation and that Incidents relating to the environment e.g. power are resolved by end customers and such Incidents are not raised as Incidents with Nasstar.
- Provide local resource to assist in Incident resolution at end customer premises where appropriate e.g. to reboot Communications Infrastructure and / or Nasstar's Equipment.
- Ensure access is available where there is a requirement for Nasstar personnel to attend site including appropriate escorts where required to meet end customer security policy.
- Use reasonable endeavours to provide a secure location with controlled access for any on site spares and access to Nasstar personnel where required to resolve an Incident.
- Ensure that any media that has been provided to ICo or the end customer as part of an installation or upgrade of any Software including associated licence keys are available at all sites where Communications Infrastructure is located.

Customer incidents may be due to failures of local facilities, eg power cuts or inadvertent removal of power from Nasstar or BT CPE, for which Customer are responsible to provide.

Before raising an edge site incident with Nasstar, the Customer will have:

1) Confirmed that more than one user is affected

2) Confirmed whether external factors could be causing a disruption to service (eg. building works)

3) Confirmed that there is power to Customer and Telco equipment

4) Confirmed that the customer can ping the LAN default gateway

5) Confirmed that the customer LAN interface router is correctly, and securely connected to the Nasstar Customer premises equipment

In addition, the Customer will supply the following information:

- The incident logging information described in section 5.2
- Symptoms of the issue (slow, intermittent, complete outage)
- Site access details (including site contact details)

For additional information refer to the "Nasstar emPSN Schools Self Triage Guide" document located on the emPSN Customer Portal.

Incidents raised by Nasstar

Nasstar will monitor edge site CPE routers for availability, and should an edge CPE router become unreachable from the exchange switch in the absence of any incident at the exchange, the incident will be referred to the Customer to undertake the initial checks above.

APPENDIX 3 – NASSTAR CNOC TEAM ORGANISATION